Written evidence submitted by Dr Tine Munk (DIS0008)

Foreign disinformation and manipulation campaigns: expert witnesses give evidence

Written Evidence submitted by Dr Tine Munk and Nottingham Civic Exchange

Executive Summary

This submission builds on research developed by Dr Tine Munk from Nottingham Trent University within this submission we argue:

- The United Kingdom (UK) faces significant threats from state and non-state actors using disinformation campaigns to manipulate public perception, destabilise democratic institutions, and undermine national security. Together with the extended use of troll farms and trolling factories to promote the falsehoods, the Russian disinformation strategy remains a significant concern.
- Our research into memetic warfare has highlighted this issue, with both counter-disinformation actors and ordinary citizens recognising its impact – but also the current gaps. Building information resilience is crucial in empowering citizens to assess information sources critically. Initiatives focusing on media literacy can help the public identify and resist disinformation, strengthening the societal fabric against malign influence.
- The rise of politically charged podcasts, blogs and Substack influencers further accelerates this shift to unregulated, direct communication, reinforcing populist movements that reject evidence-based policymaking. Disinformation spreads rapidly across TikTok, X, Reddit, and Telegram, with encrypted apps like Telegram and WhatsApp making it hard to monitor. Fringe platforms such as Gab, Truth Social, and the Chans remain key hubs for conspiracy theories, while gaming platforms like Steam, Xbox, Discord, and Twitch serve as conduits for disinformation, spreading content via text, voice chats, and live streams.

About the authors

1. Dr Tine Munk is a senior lecturer and leading researcher in memetic warfare, cyber warfare, and political communication, serving as Principal Investigator for BA-Funded project, *The Complex Web in Memetic Warfare*, at Nottingham Trent University (NTU) and Aarhus

University (AU), Denmark. She explores defensive memes, information disorder, and cyber conflicts, with key publications including *The Rise of Politically Motivated Cyber Attacks, Far-Right Extremism Online*, and *Memetic War: Online Resistance in Ukraine*. Dr Munk has made significant contributions to academic and policy discussions on digital resistance and disinformation, publishing extensively on cybercrime, cyber warfare, social media, and memetic warfare. Email: tine.munk@ntu.ac.uk.

2. Nottingham Civic Exchange is Nottingham Trent University's pioneering civic think tank. With a primary focus on issues relating to the city and the region, Nottingham Civic Exchange will enable discovery by creating a space where co-produced approaches are developed to tackle entrenched social issues. Nottingham Civic Exchange supports the role of NTU as an anchor institution in the city and the region. Nottingham Trent University holds engagement with communities, public institutions, civic life, business and residents at the core of its mission. You can find out more about our work at www.ntu.ac.uk/nce.

Submission

What are the actual and perceived threats to the UK and UK interests from state and non-state actor disinformation campaigns?

States: China, Russia, and Iran engage in systematic disinformation campaigns to undermine UK democracy, elections, and foreign policy, using social media manipulation, cyberattacks, and propaganda as part of broader hybrid warfare strategies. These efforts seek to destabilise the UK and other Western democracies by exploiting polarising issues such as immigration, the economy, and public health crises, such as Covid-19 and vaccine information. China employs covert influence operations to shape UK policy by targeting politicians and business elites. At the same time, Iran spreads anti-UK disinformation through fake social media accounts and state media, fuelling domestic unrest. With its strong ties to Russia, Iran could pose an increasing future disinformation threat to the UK.

Russia remains one of the most aggressive disinformation actors, using bot networks, cyberattacks, and state-controlled media to influence UK politics, including during UK elections and protests. Russian disinformation also fuels anti-immigrant rhetoric, as seen in false claims about the Southport tragedy, which escalated social tensions. Russia has been identified as a key player in deploying disinformation strategies to manipulate UK elections and referendums, including the 2016 Brexit vote and the 2024 parliamentary election – The Doppelgänger campaign, a Russian-backed disinformation initiative, has targeted multiple European and the United States (US) presidential

elections (2024). This campaign showcases the immediate threat by using influencers and fake accounts to amplify disinformation online.

Non-states: Disinformation is no longer the preserve of state actors. Extremist groups, conspiracy theorists, and individuals pursuing financial or ideological gain now play a major role in spreading false information. Advances in AI and the weakening of content moderation on social media have made it easier to manipulate public opinion on a large scale. The 2024 UK riots showed how online platforms allowed far-right extremists to distribute disinformation to thousands, which fuelled the unrest. The threat comes not just from organised extremist leaders but also from ordinary citizens who knowingly or unknowingly spread falsehoods that undermine trust in UK institutions and the police.

Extreme far-right and populist movements, including groups linked to the US Make-America-Great-Again (MAGA) movement and QAnon, use social media, memes, and podcasts to push misleading narratives and exploit societal divisions. Religious extremists have long used disinformation to destabilise societies, and extreme far-right groups and actors now mirror these tactics by adopting methods to confuse and manipulate online users. Conspiracy theorists and ideological agitators also exploit digital platforms to erode public trust, while troll farms and private entities amplify falsehoods—many with close links to states/ following state strategies. Russian-backed networks blur the line between public and private actors, by using different actors to spread fabricated narratives, such as the former Russian troll farm, the Internet Research Agency (IRA). Groups and individuals that previously were hiding online have now moved into mainstream social media, where anonymity is no longer required. Engagement-driven algorithms prioritise sensational content, making hate speech and disinformation visible.

What are the actual and perceived threats to Europe, the Americas, Indo-Pacific and Africa from state-sponsored disinformation campaigns targeting democratic values and institutions?

During the 2024 European Parliament elections, Russian-linked networks spread anti-EU narratives and bribed MEPs to weaken support for Ukraine. Similar tactics influenced Finland's 2024 presidential election, where false claims and fake posters sought to discredit candidates, and Germany's 2025 elections, where Russian bots fabricated terror threats to suppress voter turnout. Eastern European states like Moldova, Georgia and Romania have been targeted by pro-Kremlin disinformation favoured Russian-aligned candidates, triggering unrest. Beyond elections, disinformation destabilised key events, such as the 2024 Paris Olympics, where Russia fabricated Hamas-linked terror threats to erode public confidence. Operation Doppelgänger spread anti-Zelenskyy narratives in Germany and France, while leaked records expose Russian efforts to promote extreme far-right EU parties.

The US remains a key target, with Russia leading influence operations to undermine trust, interfere in elections, and polarise the population. The Social Design Agency behind Doppelgänger launched 'The Good Old USA Project' in 2023, influencing the 2024 US election by amplifying domestic issues like inflation instead of directly backing pro-Russian candidates. The campaign targeted

minority communities, swing-state voters, and online gaming platforms, shifting attention away from US support for Ukraine to weaken bipartisan backing for sanctions and military aid. Russian disinformation impersonates major Western media, including The Guardian, Der Spiegel, The Washington Post, and Fox News, while Storm-1516, an IRA offshoot, runs troll farms and bot networks. War on Fakes, disguised as a fact-checking site, spreads pro-Kremlin propaganda, threatening US national security with tactics seen across Western democracies.

In the Indo-Pacific, state and non-state disinformation campaigns shape public perception and policy, often benefiting authoritarian interests. China has been linked to cyberattacks and election interference, notably in the 2019 Australian election, and has intensified influence operations in the Philippines since 2023. In September 2024, an image from a 2017 US-Japan military drill was falsely presented as a US-China standoff in the South China Sea. Beyond China, nationalist-linked disinformation fuels Indian political campaigns, while in Indonesia, false narratives divide the population and deflect scrutiny. Pakistani-linked accounts weaponised immigration, spreading false claims that Donald Trump planned to deport 18,000 Indian immigrants, straining US-India relations.

In Africa and the Middle East, state-sponsored disinformation serves as a tool for geopolitical influence, with Russia, China, the United Arab Emirates, Saudi Arabia, and Qatar using false narratives to undermine democracy and challenge Western policies. Russian operatives create fake news outlets and impersonate media to spread pro-Kremlin propaganda, destabilising political landscapes. Since Russia's 2022 invasion of Ukraine, its campaigns have blamed the West for economic hardship and food insecurity, seeking to weaken sanctions and interfere in regional conflicts. In the Middle East, Russian Arabic-language disinformation fuels conspiracy theories and manipulates public opinion, expanding Russia's influence beyond Europe.

Who are the main state and non-state actors spreading disinformation?

State actors: Russia, China, Iran, and the US are using different types of methods, such as state-controlled media, troll farms, online communications, and cyber operations to advance their geopolitical agendas. Russia poses the greatest threat, systematically deploying disinformation campaigns and influence networks to spread its narratives globally. While the new US administration's approach to facts and fact-checking appears less coordinated than the structured efforts of Russia, China, and Iran, it still shapes public perception of truth and influences the understanding of disinformation, further muddying the information landscape and enabling false narratives to spread unchecked.

China shapes global narratives about Taiwan, the Philippines, Hong Kong, and Western democracies using state-controlled media like Global Times, Xinhua, and China Global Television Network, alongside TikTok, which serves as a powerful tool for disinformation. China spreads pro-Beijing narratives in the UK and Europe through media manipulation, social media campaigns, and covert influence operations. Tactics include 'Spamouflage' networks, which mix unrelated content with disinformation, and intelligence-linked groups like the United Front Work Department, which infiltrate UK political circles to influence lawmakers and business elites. China's disinformation

strategy seeks to shape public opinion, undermine Western narratives, and expand its geopolitical influence.

Iran spreads anti-US and anti-Israel disinformation, using fake news outlets and digital influence operations to manipulate public opinion. Iran's Islamic Revolutionary Guard Corps has interfered in US elections, engaging in cyberwarfare tactics against the US. Following the Southport tragedy, Iran-linked networks also amplified false claims online. Meanwhile, Press TV, Iran's state-run broadcaster, continues to push anti-UK narratives and air forced confessions. These actions highlight Iran's ongoing efforts to destabilise Western politics.

Alongside President Putin and Foreign Minister Lavrov, Russia's disinformation operations are driven by key figures within the Presidential Administration, the Ministry of Foreign Affairs, and state-controlled media. Kiriyenko, First Deputy Chief of Staff, directs foreign influence campaigns, including election interference. Zakharova, the Foreign Ministry's spokesperson, amplifies Kremlin narratives, while Peskov, Putin's Press Secretary, controls state propaganda and media messaging. At the UN, Ambassador Nebenzya defends Kremlin disinformation, distorting facts about Ukraine and Western policies. These officials coordinate influence operations through state-run media, diplomatic channels, and online propaganda networks to manipulate global opinion and advance Russia's geopolitical goals. However, they represent only a fraction of the vast disinformation apparatus, which operates at multiple levels, including pro-Russian actors and Western political influencers.

Non-State Actors: Troll farms in Russia, China, and Iran use bot networks and meme campaigns to spread false narratives and manipulate public opinion. Russia's Doppelgänger campaign impersonates media outlets to distribute disinformation, making its full reach difficult to track. These operations, often privately funded but government-directed, blur the line between state and non-state actors, enabling covert influence and election interference.

Russia's state-controlled media is led by key propagandists shaping domestic and international narratives. Kiselyov (Rossiya Segodnya) and Simonyan (RT) push pro-Kremlin and anti-Western messaging, while Solovyov promotes hardline nationalism and inflammatory rhetoric. Poddubny amplifies military propaganda, Skabeyeva aggressively defends Kremlin policies, and Trofimova has faced criticism for sympathetic portrayals of Russian soldiers. These figures drive Russia's disinformation efforts, using TV, digital media, and social platforms to reinforce state narratives.

Under Musk's control of X, the social media company has weakened content moderation, allowing far-right disinformation and conspiracy theories to spread unchecked. Major media outlets have left X over rising disinformation and weak moderation, reflecting concerns about Musk's ties to the Trump administration and his unverified political claims that blur fact and fiction, such as his backing of Germany's Alternative für Deutschland (AfD), spreading disinformation during the UK election and 2024 riots, and amplifying false claims on migration and unrest—actions condemned by UK officials amid concerns over foreign influence. X remains a key platform for the UK government and its officials, offering access to a large audience and the ability to counter disinformation. However, staying on X also risks legitimising extremism and disinformation, undermining credibility, and raising security concerns due to its weak moderation. The challenge is whether the

benefits of engagement outweigh these risks or if it is time to shift to less problematic platforms like BlueSky.

The current US President's use of Truth Social has amplified extreme far-right narratives, spreading election fraud conspiracies, promotes falsehoods and disinformation, pro-Putin propaganda, and deep-state theories. Key figures in the MAGA movement, including politicians such as Vice President Vance, Gaetz, Taylor Greene, Boebert, etc. have pushed false narratives and conspiracy theories, mirroring Russian disinformation tactics to undermine institutions, relationships, practices, and processes.

In the United Kingdom, extreme far-right and far-left campaigns have strong ties to Russia. Figures like Robinson have spread inflammatory, misleading content targeting immigrants, while Galloway's 2024 campaign was boosted by bot networks linked to Russia or China and echoed Kremlin disinformation. Similar patterns emerge in Europe, with Le Pen (Rassemblement National) in France and Weidel (AfD) in Germany promoting pro-Kremlin narratives and maintaining close ties to Musk. This highlights the role of state-backed and ideological actors in destabilising democracies through disinformation.

What channels and technologies are state and non-state actors using to spread disinformation?

Disinformation campaigns use AI, social media, and encrypted messaging apps to manipulate public opinion and destabilise democracies. AI-generated deepfakes and fake news generators create fabricated videos, audio, and articles to influence elections and public discourse. In October 2023, a deepfake of Labour leader Starmer swearing at staff highlighted the UK's vulnerability to AI-driven disinformation, a tactic also used in the 2024 US presidential election with fabricated footage of politicians spreading false claims.

Memes have become a key disinformation tool, used both to attack individuals and influence political events. Memetic warfare, as defined by Munk (2024), is a form of information warfare using memes for political, strategic, or ideological goals. Disinformation memes spread falsehoods through humour and satire or are used aggressively to manipulate public opinion, as seen in elections in the US, UK, France, and Germany. Pro-MAGA meme pages like DC Draino, RagingAmericans, Snowflaketears and The Typical Liberal, etc., act as disinformation hubs, reaching millions on Instagram and X. This trend has expanded globally, influencing UK politics and beyond.

Social media platforms amplify disinformation, as engagement-driven algorithms prioritise sensational content over accuracy. The 2024 Romanian presidential election demonstrated this, with pro-Russian candidate Georgescu's success linked to a TikTok-driven disinformation campaign. Troll farms, bot networks, and influencers further boost false narratives. Leaving social media unmoderated and without fact-checking allows disinformation to thrive unchecked.

Recommendations:

The effectiveness of cross-departmental and inter-governmental coordination, alongside the private sector in countering state-sponsored disinformation?

1. **Enhancing inter-governmental collaboration for effective policies**

The UK collaborates internationally to combat disinformation, sharing intelligence with the US, engaging in post-Brexit security initiatives with the European Union (EU), and working with Commonwealth allies such as Australia and Canada to expose Russian influence operations and manipulations. It has signed the Council of Europe (CoE) Framework Convention on Artificial Intelligence to address AI-driven disinformation and supports United Nations (UN) efforts to counter global misinformation on climate change and political stability. Domestically, the UK has launched initiatives. For example, the National Security and Online Information Team that works with intelligence agencies and regulators. While these efforts are crucial, disinformation threats from adversary states continue to evolve, demonstrating that current measures remain insufficient to counter foreign influence operations fully.

2. **Legislation is a pillar of effective governance**

The UK works with social media platforms and fact-checking organisations to flag and mitigate misleading content. The Online Safety Act 2023 aims to hold tech companies accountable. But there needs to be a much more assertive approach to this area, like the EU Digital Services Act. Enforcement remains challenging due to platforms reducing moderation efforts, such as X's (former Twitter) rollback of content policies and Meta's decision to end third-party fact-checking in the US, with potential spillover effects in Europe. Closer collaboration with social media companies is essential, as their platforms serve as primary channels for disinformation. The reduction in fact-checking and moderation has weakened efforts to combat false narratives, making it harder to contain and stop misleading content.

3. **Investing in research is key to closing the disinformation gap**

A critical gap in the UK's disinformation response is insufficient funding for academic research. While initiatives such as the Bilateral Academic Research Initiative provide valuable resources, the current funding mechanisms for national small and large-scale projects are too slow, limiting the ability of researchers to respond to emerging threats in real-time. More funding - timely and streamlined access to grants - is essential to support long-term studies on disinformation tactics, state-

backed influence operations, and effective countermeasures and strategies. Without this, the UK risks falling behind in developing evidence-based strategies to combat digital manipulation.

Despite progress in cross-government coordination, enforcement is hindered by shifting platform policies, private sector resistance, and evolving disinformation tactics. The UK must expand media literacy, invest in research, and hold tech companies accountable, while also leading efforts to regulate AI-generated content, including deepfake visuals, videos, and audio used in disinformation campaigns. Sustained government and industry collaboration is essential to close enforcement gaps and strengthen resilience.

What lessons can the UK learn from allies in countering state-sponsored disinformation targeting democratic values and institutions?

4. **Strengthening international cooperation**

The UK could benefit from developing international cooperation to counter foreign disinformation through intelligence-sharing and coordinated responses. For example, use a structure similar to the now-terminated US Global Engagement Centre (GEC) to strengthen international initiatives and ensure a robust response to malign influence operations while maintaining transparency and democratic accountability. Proactive measures, such as publicly exposing nascent disinformation efforts before they gain traction, have been effective. In the past, the US GEC revealed covert operations early, disrupting their potential impact.

5. **Using AI for disinformation detection**

NATO emphasises the use of AI tools to identify and mitigate the spread of false and harmful content. By developing and investing in AI and other advanced technologies, the UK can improve its capacity to detect and counteract disinformation campaigns effectively. The UK could adopt AI strategies to stay ahead of adversarial narratives and become world-leading in the fight against disinformation. The Cold War era offers insights into countering disinformation, highlighting the importance of robust public communication and strategic information dissemination to combat false narratives. Reflecting on these historical strategies can inform contemporary approaches to disinformation using new technology.

6. **Learning from grassroots activism**

Online grassroots groups play a crucial role in countering malign actors' disinformation, using grassroots digital activism to defend democratic values. Lithuania's Elves combat pro-Kremlin propaganda, debunking false narratives across Central and Eastern Europe. Ukraine's IT Army disrupts Russian digital infrastructure and spreads accurate conflict-related information. The North Atlantic Fella Organization (NAFO), a global online network, uses memetic warfare to expose pro-Russian disinformation while raising support for Ukraine. The UK can learn from these groups as they demonstrate how community-driven initiatives can effectively challenge malign influence operations on social media.

20 February 2025